REMARKS

Favorable reconsideration of this application as presently amended and in light of the following discussion is respectfully requested.

Claims 2, 5, 6, 9, 10, and 14-23 are pending in this application, Claim 3 having been cancelled without prejudice or disclaimer; Claims 1, 4, 7, 8, and 11-13 having previously been canceled without prejudice or disclaimer; and Claims 2, 5, 9, and 23 having been amended. Support for amended Claims 2, 5, 9, and 23 can be found, for example, in the original claims, drawings, and specification.[1] No new matter has been added.

In the outstanding Office Action, the claims were objected to due to informalities; Claims 2, 3, 5, 6, 9, 10, and 14-23 were rejected under 35 U.S.C. § 103(a) as unpatentable over Subramaniam et al. (U.S. Patent No. 6,081,900; hereinafter "Subramaniam") in view of Katano Guthrie et al. (U.S. Patent No. 6,606,627; hereinafter "Katano Guthrie").

In response to the objection to Claim 9, Applicants have amended Claim 9 in accordance with the suggestions set forth in the outstanding Office Action. Accordingly, Applicants respectfully submit that the objection to Claim 9 has been overcome.

In response to the rejection of Claims 2, 3, 5, 6, 9, 10, and 14-23 under 35 U.S.C. § 103(a) as unpatentable over Subramaniam in view of Katano Guthrie, Applicants respectfully submit that amended independent Claim 2 recites novel features clearly not taught or rendered obvious by the applied references.

Amended independent Claim 2 is directed to a database access control method including, *inter alia*:

> ... generating, in the database access control apparatus when sending the address of the proxy process server apparatus to the user apparatus, an access key based on a user ID of the user apparatus, storing the access key and a server ID of the proxy process server apparatus in a storing part of the database

[1] See page 10, line 25 to page 12, line 14 of the specification.

> access control apparatus associating the access key with the server ID and sending the access key and the address to the user apparatus;
>
> sending, in the user apparatus, the access key to the proxy process server apparatus when making the database access request to the proxy process server apparatus;
>
> sending, in the proxy process server apparatus, the access key and the server ID of the proxy process server apparatus to the database access control apparatus when making the database process request to the database access control apparatus; and
>
> determining, in the database access control apparatus, whether an access key the same as the access key received from the proxy process server apparatus exists in the storing part, if the access key exists in the storing part, determining whether an ID, associated with the access key, that is the same as the server ID received from the proxy process server apparatus exists in the storing part, and executing an access to data in the database within a limit permitted for the user ID corresponding to the access key only if the server ID exists in the storing part.

Independent Claims 5, 9, and 23 recite substantially similar features as Claim 2. Thus, the arguments presented below with respect to Claim 2 are also applicable to independent Claims 5, 9, and 23.

Page 6 of the outstanding Office Action asserts that Subramaniam describes "determining, in the database access control apparatus, whether an access key the same as the access key received from the proxy process server apparatus exists in the storing part (see e.g. col. 8 lines 47-57 and col. 11 lines 65-67 and col. 12 lines 33-46, note that border server notify user if 'access key' refers as user name and password' are validated by the authentication system within the secure network) and executes an access to data in the database within a limit permitted for the user ID corresponding to the access key only if the access key exists in the storing part."

However, Subramaniam fails to teach or suggest "determining, in the database access control apparatus, ***whether an access key the same as the access key received from the proxy***

process server apparatus exists in the storing part, if the access key exists in the storing part, determining whether an ID, associated with the access key, that is the same as the server ID received from the proxy process server apparatus exists in the storing part, and executing an access to data in the database within a limit permitted for the user ID corresponding to the access key only if the server ID exists in the storing part," as in Applicants' Claim 2.

Subramaniam describes that a user enters a user name and a corresponding password in fields shown on a login screen. The username and password are then transmitted over a secure connection to a border server 106, which passes the user name and password to an authentication system with the secure network 100. If the username and password are validated by the authentication system, the border server 106 so notifies the user and the user is then granted access to secure network data.[2] However, in Subramaniam, the border server 106 does not determine whether an access key (the same access key received from a proxy process server apparatus) exists in the authentication system, and if the access key exists in the authentication system, determine whether an ID, associated with the access key, that is the same as a server ID received from the proxy process server apparatus exists in the authentication system. In other words, Subramaniam does not describe determining whether ***an access key and an ID of the proxy process server apparatus*** exists in a storing part of a database access control apparatus.

Further, problems arise when a proxy process server (e.g. border server 106 of Subramaniam) is not located in a secure network. That is, even though session capability is effective for management after identifying the user, problems, such as those described at pages 3-4 of Applicants' Background Art section of the specification, arise when the proxy process server does not have enough credibility (i.e., when the network is not secure) to

[2] See Subramaniam at column 8, lines 47-57.

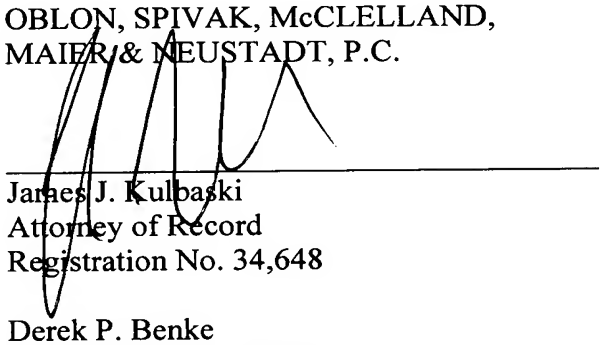
perform certain processes. However, in the database access control method of Applicants' Claim 2, secure processing can be realized even when the network is not secure due to processes performed in the database access control apparatus and the proxy process server apparatus using the session key and the ID of the proxy process server apparatus.

Accordingly, Applicants respectfully request that the rejection of Claims 2, 3, 5, 6, 9, 10, and 14-23 under 35 U.S.C. § 103(a) as unpatentable over Subramaniam in view of Katano Guthrie be withdrawn.

Consequently, in view of the present amendment, and in light of the above discussion, the pending claims as presented herewith are believed to be in condition for formal allowance, and an early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



James J. Kulbaski
Attorney of Record
Registration No. 34,648

Derek P. Benke
Registration No. 56,944

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413-2220
(OSMMN 03/06)

I:\ATTY\DPB\26's\265122US\265122US-AM2.DOC